UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v.-

JOSHUA ADAM SCHULTE,

Defendant.

S1 17 Cr. 548 (PAC)

STATE OF NEW YORK)
COUNTY OF NEW YORK ss.:
SOUTHERN DISTRICT OF NEW YORK)

I, LUIS CRUZ, pursuant to Title 28, United States Code, Section 1746, declare under penalty of perjury:

1. I am a computer scientist with the Federal Bureau of Investigation ("FBI") and have been so employed since 2015. I am currently assigned to a squad responsible for conducting investigations into cybercrime. Through my training and experience, I am familiar with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. Beginning in or about mid-April 2017, I, along with other computer scientists, was involved in forensically analyzing electronic devices seized from the residence of the defendant Joshua Adam Schulte pursuant to various search warrants (the "Electronic Devices"). When I joined the investigation, I was aware that the FBI had obtained a warrant to search the Electronic Devices for evidence of espionage and related offenses, in connection with the disclosure of classified information by WikiLeaks.org that began in March 2017 (the "Espionage Warrant"). I was also aware that prior to my joining the investigation, the FBI had briefly stopped reviewing the Electronic Devices upon discovering evidence of, among other

things, child pornography on Schulte's desktop computer (the "Desktop Computer"), and that the FBI started searching the Electronic Devices again only after obtaining another warrant authorizing the seizure of evidence related to child pornography and copyright infringement offenses (the "Supplemental Warrants"). I reviewed the Espionage Warrant and Supplemental Warrants before I started reviewing the Electronic Devices.

3. When I joined the investigation, I was initially tasked with reviewing the Desktop Computer. Based on my review of Schulte's Desktop Computer and my conversation with other computer scientists, I am aware that the Desktop Computer contained four storage devices, three of which were configured as an encrypted Raid 5 volume, that is, a data storage system that combines multiple drives into one unit for, among other things, data redundancy (the "Raid 5 Volume"). I am also aware that the Raid 5 Volume was decrypted by other FBI personnel who were able to, among other things, extract the decryption key from the Desktop Computer.

4. Within the Raid 5 Volume, there was an approximately 100 gigabyte of space allocated to an encrypted Linux Mint Virtual Machine (the "VM"). In general, a virtual machine is a full computer system within a physical computer. I was able to defeat the full disc encryption of the VM by inputting a password ("Password-1"). Based on my conversations with others, I am aware that Password-1 was obtained based on a forensic examination of other of the Electronic Devices (the "Forensic Examinations"), which reflected that Schulte used Password-1 for other of his accounts.

5. After defeating the full disc encryption of the VM, I discovered a user account "josh" with a password protected home directory (the "Home Directory"). I was able to log into and access the Home Directory by inputting a different password obtained from the Forensic Examinations ("Password-2").

6. Upon accessing the Home Directory, I identified a file titled "data.bkp" that was approximately 50 gigabytes in size (the "Data File"). Initially, when I opened the Data File, the file appeared to contain a high degree of randomness. However, I determined that an encryption software called VeraCrypt was installed on the VM. VeraCrypt allows users to create encrypted, password protected containers (*e.g.*, zip files) on their computers. Based on the size of the Data File and its contents, which appeared to be highly random data, and based on the presence of VeraCrypt on the VM, I determined that the Data File was potentially a VeraCrypt encrypted container.

7. On or about April 20, 2017, I was subsequently able to decrypt the Data File using VeraCrypt Software by entering Password-1—that is, the same password used to access the VM. Once the Data File was decrypted, it was immediately apparent to me from the names of the files that many likely contained child pornography. Exhibit A to my declaration is a screenshot of the decrypted Data File showing the folder structure on the left side of the screen. As reflected on Exhibit A, the folder names included, among others, "11yr old"; "13YO IN BATH"; and "kids." The other portion of Exhibit A shows the names of some of the files within the folder titled "new." The file names include, among others, "(PTHC) Kelly 8Y0 – Sucking & Trying Fuck.avi"; "(pthc) TF-BTF-01 – Man Gets In Bed With Hot 7yo.mpg"; and "3+4yr 2 Girls children sexually abused BEAUTIFUL_Venezuela part-2 .mpg".

8. After decrypting the Data File and observing file names that appeared to indicate child pornography, I and another computer scientist promptly contacted FBI Special Agent Richard J. Evanchec, who at the time was one of the case agents in charge of the investigation. After consulting with Special Agent Evanchec, I opened several of the files, which appeared to me to contain child pornography.

9. In addition, within the Data File, there was an additional file also titled "data.bkp" that was several gigabytes in size and that also contained a high degree of randomness (the "Second Data File"). I was able to decrypt the Second Data File using VeraCrypt Software by entering the same password used to defeat the full disc encryption of the VM and to access the Data File, as described above. Once the Second Data File was decrypted, it contained forensic artifacts of files having names indicative of child pornography.

10. After I identified and decrypted the Data File and Second Data File, I and other computer scientists also identified within the Raid 5 Volume another VeraCrypt encrypted container titled "volume," which appeared to contain over approximately 100 gigabytes of data (the "Volume Encrypted Container"). Once the Volume Encrypted Container was decrypted, it contained, among other things, additional images and videos (the "Additional Child Pornography"). I understand that the Additional Child Pornography was reviewed by members of the FBI's Crimes Against Children Squad who determined that it was, in fact, child pornography.

11. In accessing the foregoing locations on the Desktop Computer, I did not use any forensic techniques, such as keyword searches, directed to identifying child pornography. Rather, my focus in reviewing the Desktop Computer was to unlock and review hidden, encrypted, and/or password protected portions of the Desktop Computer to identify evidence of the espionage offenses. Based on my training, experience, and participation in this and other investigations, I believed that the Data File, Second Data File, and Volume Encrypted Container were likely to contain evidence of the espionage offenses based on their location, size, and encryption, and I would have attempted to decrypt and review the files in those locations pursuant to the Espionage Warrant whether or not I was also authorized to review the Desktop Computer for evidence of child pornography.

12. I declare under penalty of perjury that, to the best of my knowledge, the foregoing information is true and correct.

Dated: New York, New York
August 2, 2019

Luis Cruz
Computer Scientist
Federal Bureau of Investigation